Secure Transmission in Linear Multihop Relaying Networks

Jianping Yao, Xiangyun Zhou, *Senior Member, IEEE*, Yuan Liu, *Member, IEEE*, and Suili Feng, *Member, IEEE*

***Abstract*—This paper studies the design and secrecy performance of linear multihop networks, in the presence of randomly distributed eavesdroppers in a large-scale two-dimensional space. Depending on whether there is feedback from the receiver to the transmitter, we study two transmission schemes: on-off transmission (OFT) and non-on-off transmission (NOFT). In the OFT scheme, transmission is suspended if the instantaneous received signal-to-noise ratio (SNR) falls below a given threshold, whereas there is no suspension of transmission in the NOFT scheme. We investigate the optimal design of the linear multiple network in terms of the optimal rate parameters of the wiretap code as well as the optimal number of hops. These design parameters are highly interrelated since more hops reduces the distance of per-hop communication which completely changes the optimal design of the wiretap coding rates. Despite the analytical difficulty, we are able to characterize the optimal designs and the resulting secure transmission throughput in mathematically tractable forms in the high SNR regime. Our numerical results demonstrate that our analytical results obtained in the high SNR regime are accurate at practical SNR values. Hence, these results provide useful guidelines for designing linear multihop networks with targeted physical layer security performance.**

***Index Terms*—Physical layer security, linear multihop network, homogeneous Poisson point process (PPP), randomize-and-forward (RaF) relaying.**

I. Introduction

A. Background and Motivation

With the rise of the Internet of Things (IoT), the need for wireless networks that offer a wide variety of quality-of-service (QoS) features is fast growing. It becomes clear that guaranteeing reliable and secure transmission are two major issues. Due to wireless signal attenuation with transmission distance, cooperative relaying has been considered as an effective method to increase the range and reliability of wireless networks. Several relaying strategies have been adopted in major wireless standards. At the same time, due to the broadcast nature of wireless channels, wireless communication is subject to a wide range of security threats. Traditionally, security risks have been addressed at the upper layers of the wireless network protocol stack. More recently, physical layer security is emerged as a new and complementary security solution that exploits the physical characteristics of the wireless channel from an information-theoretic point of view.

For two-hop wireless networks, there exists abundant research publications considering the physical layer security for wireless networks, e.g., [1–4]. Early studies, such as [1], investigated how to achieve physical layer security with the conventional relaying schemes like decode and forward (DF) and amplify and forward (AF). New cooperation strategies like cooperative jamming (CJ) were also introduced as secrecy enhancements. When designing the two-hop network, the power allocation and rate adaptation were important parameters to optimize. Relay selection was also an effective way of improving the secrecy performance when multiple potential relays are available. The modeling of the node locations, e.g., for a network having multiple potential relays and multiple eavesdroppers, were done either deterministically or statistically using stochastic geometry tools.

While the aforementioned works focused on two-hop relaying systems, it is worth investigating the secure communication in more elaborate networks, which take more than two hops. However, extending the analysis from two-hop networks to multihop networks is non-trivial, because more hops means that more nodes are involved in the transmission as well as more chances for eavesdropping. In addition, the number of hops becomes a design parameter affecting the end-to-end delay and hence throughput. In this work, we study the interesting but challenging scenario of multihop relaying networks.

B. Related Work and Novelty of Our Study

Only a few studies have addressed the physical layer security in multihop relaying systems [5–12]. Among these works, the majority of them addresses the secure routing design with various considerations. For example, the authors in [5] proposed a tree-formation game to choose secure paths in uplink multihop cellular networks. The authors in [6, 7] considered minimum energy routing in the presence of either multiple malicious jammers or eavesdroppers, to guarantee certain end-to-end performance. The authors in [8, 9] considered the problem of how to communicate securely with the help of untrusted relays and full-duplex jamming relays, respectively. The authors in [10] addressed the secure routing problem in multihop wireless networks with half-duplex DF relaying,

Manuscript received April 11, 2017; revised September 10, 2017; accepted October 30, 2017. This paper was supported in part by the Natural Science Foundation of China under Grant 61401159 and Grant 61771203, in part by the Pearl River Science and Technology Nova Program of Guangzhou under Grant 201710010111, and in part by the Guangdong Science & Technology Plan under Grant 2016A010101009. The work of X. Zhou was supported by the Australian Research Council Discovery Projects under Grant DP150103905. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. A. Zaidi.

J. Yao, Y. Liu, and S. Feng are with School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510641, China (e-mails: yaojp_scut@qq.com, eeyliu@scut.edu.cn, fengsl@scut.edu.cn).

X. Zhou is with the Research School of Engineering, The Australian National University, Canberra, ACT 0200, Australia (e-mail: xiangyun.zhou@anu.edu.au).

where the locations of the eavesdroppers were modeled as a homogeneous Poisson point process (PPP).

By reviewing the existing studies on multihop wireless networks, we see that there is some knowledge gap at a fundamental level. Questions like what is the optimal number of hops for a given pair of source and destination is largely an open problem. Although the prior studies on secure routing have somewhat addressed this problem for given network configurations, the focus there was to find the best route for given locations of intermediate nodes, instead of directly analyzing the optimal number of hops when the network allows one to deploy the relays or to select relays from a large pool of available nodes. In addition, it is unclear how the optimal design of secure transmission at each hop is affected by the number of hops.

To the best of our knowledge, only one recently published work in [13] directly addressed the knowledge gap identified above. Specifically, this work considered a linear multihop network in the presence of randomly distributed eavesdroppers and addressed the question of the optimal number of hops. Deviating from the most common physical-layer-security approach of using wiretap code, the work in [13] adopted ordinary code that does not provide any level of information-theoretic secrecy. Without wiretap code, the legitimate users have a significantly reduced level of control over the secrecy performance when designing their transmission strategy. In contrast, we consider the use of wiretap code and define secrecy performance from an information-theoretic viewpoint as commonly done in the literature of physical layer security. In this way, the design of the wiretap coding rates has direct impact on both the throughput performance and the secrecy performance. Therefore, the novel contribution of our work is the obtained design guideline on the transmission strategy and number of hops in securing a multihop relaying network with wiretap code protection. As will be discussed, the design guidelines obtained with wiretap code (i.e., this work) and without wiretap code (i.e., [13]) are very different.

C. Our Approach and Contribution

In this paper, we study the problem of secure transmission design in a linear multihop wireless network in the presence of randomly distributed eavesdroppers whose locations are modeled using a homogeneous PPP. The relays adopt the randomize-and-forward (RaF) relaying protocol where each relay generates the transmitted codeword independently so that secrecy of individual hops guarantees the secrecy of the entire path [14]. The celebrated wiretap code is used to provide the desired physical layer security. We attempt to answer a fundamental question: If the network allows one to deploy equally-spaced relays or to select equally-spaced relays from a large pool of available nodes in a dense network, what is the optimal number of hops and what is the corresponding optimal design of the coding rates for achieving the best physical layer security performance? To answer this question, we formulate a throughput maximization problem with an end-to-end secrecy outage probability constraint. Solving the problem is a non-trivial task because the design parameters are highly interrelated. Having more hops reduces the per-hop communication distance, meaning that a higher rate can be used. On the down side, more hops not only increases the total time for communication but also gives the eavesdroppers more chance to intercept the message. Clearly the encoding rates of the wiretap code need to be carefully designed to achieve the best tradeoff between throughput performance and secrecy performance.

The main contributions of this paper are summarized as follows:

- Using a stochastic geometry model for the eavesdroppers' locations, we derive an analytical expression for the end-to-end secrecy outage probability, which is used to measure the secrecy performance of the multihop wireless network.
- Depending on whether there is feedback from the receiver to the transmitter, we consider two transmission schemes: on-off transmission (OFT) and non-on-off transmission (NOFT). For both schemes, we solve the throughput maximization problem under a given secrecy outage probability constraint. In particular, the optimal rate parameters of the wiretap code are obtained in mathematically tractable forms.
- We obtain further analytical insights on the optimal design parameters and the achievable throughput in the asymptotic high signal-to-noise ratio (SNR) regime. These high SNR results are actually found to be accurate at practical SNR values as verified by numerical results. Regarding the optimal number of hops, our results show that the optimal value is insensitive to the change in operating SNR. On the other hand, the optimal number of hops increases as the density of eavesdroppers increases.

It is necessary to compare our results with the ones in [13] which considered the same network scenario (but with the addition of randomly distributed interferers) and addressed the same question of the optimal number of hops. As described before, the work in [13] did not consider the use of wiretap code which is a key technique in physical layer security. Under such a framework, the main conclusions in [13] were (i) a greater number of hops are preferable to a smaller number of hops in any situation; and (ii) imposing a (more stringent) secrecy constraint does not change the maximum achievable throughput. In contrast to [13], our framework adopts wiretap code. Consequently, the achievable throughput is clearly a function of the required secrecy constraint. Regarding the optimal number of hops, our finding is certainly not "the more the merrier". For example, the optimal number of hops reduces as the eavesdropper's density reduces. To sum up, our definition of secrecy and the considered secure transmission schemes are fundamentally different from [13], which leads to very different conclusions on the optimal system design and the resulting performance. The work in [13] and our work complement each other and give different design guidelines depending on whether wiretap code is used or not.

The remainder of this paper is organized as follows. In Section II, the system model and performance metric are described. In Section III, the secrecy performance and secure

TABLE I
LIST OF NOTATION

α	Path loss exponent ($2 \leq \alpha \leq 6$)
Φ_{ne}	Poisson point process of eavesdroppers' location
λ_e	Density of Φ_{ne}
p	Transmit power
N	Number of hops
L	S-D distance
D_n	Transmission distance of nth hop
H_n	Channel fading gain of nth hop
S_{ne}	Distance of the eavesdropping channel of nth hop
X_{ne}	Channel fading gain of eavesdropping channel of nth hop
R_t	Rate of the transmitted codewords
R_s	Rate of the confidential information
R_e	Rate loss for securing the messages against eavesdropping
$\mathcal{P}_t^{'}$	Transmission probability over a single hop
$\mathcal{P}_{\mathrm{c}}^{'}$	Connection probability over a single hop
$\mathcal{P}_{\mathrm{c}}$	End-to-end connection probability over the path
$\mathcal{P}_{\mathrm{so}}^{'}$	Secrecy outage probability over a single hop
$\mathcal{P}_{\mathrm{so}}$	End-to-end secrecy outage probability over the path
ϵ	Constraint on $\mathcal{P}_{\mathrm{so}}$
β_t	SNR threshold for decoding the message correctly
β_e	SNR threshold for secrecy outage
$C_{ne}^{\max}$	Maximum capacity of eavesdropping channels of nth hop
$\mathtt{SNR}_{ne}^{\max}$	Maximum received SNR at eavesdroppers of nth hop
$\mathbb{U}$	Secure transmission throughput
$\mathcal{P}(\cdot)$	Probability operator
$\mathbb{E}(\cdot)$	Expectation operator
$\Gamma(\cdot)$	Gamma function
$\mathbb{W}_0(\cdot)$	Principal branch of Lambert W function

transmission design for a multihop path are investigated. In Section IV, the numerical results are presented. Finally, the conclusion is drawn in Section V. Table I summarizes the list of notation used in this paper.

II. System Model and Performance Metric

A. System Model

We consider a linear N-hop wireless relay network of length L as shown in Fig. 1, consisting of a source node A_1, a destination node A_{N+1} and $N-1$ relay nodes $(\{A_i\}, i = 2, \ldots, N)$, which is exposed to a set of randomly deployed eavesdroppers over a large two-dimensional area. We model the locations of the eavesdroppers in each hop as an independent homogeneous PPP with intensity λ_e denoted by $\Phi_{ne}\,(n = 1, \ldots, N)$. The eavesdroppers are non-cooperative, so they must decode the messages individually. All nodes are equipped with one omni-directional antenna and, hence, cannot transmit and receive signals simultaneously which is referred to as "half duplex". Furthermore, the transmission is performed via time-division which guarantees that there is no interference between the different hops. Node A_{n+1} only receives the signal transmitted by its adjacent node A_n.

In this paper, we assumed that the relays are equidistant with each other as in [15–17]. Such a model is mathematically tractable to investigate the impact of the number of hops and hence, is well-adopted in the literature in studying multihop network. It can be used to approximate the performance of a dense network, where we can pick approximately equidistant nodes as relays. We can also find it in practical, e.g., the communication between the electrical equipments in smart grid, or the communication between road-side units placed along the road and railway.

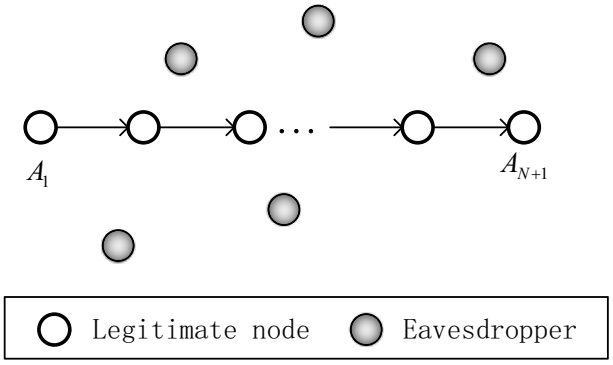


Fig. 1. An illustration of a linear multihop relaying network surrounded by several eavesdroppers. The confidential message is transmitted from the source node A_1 to the destination A_{N+1} with the help of relays $(\{A_i\}, i = 2, \ldots, N)$, and at the same time the eavesdroppers attempt to intercept the transmitted message.

All the channels are modeled by large-scale attenuation with path loss exponent α along with small-scale Rayleigh fading. We consider the non-singular (bounded) path loss model $\frac{1}{1+r^{\alpha}}$, where r denotes the communication distance [18–22]. The corresponding channel power gains are independent and exponentially distributed with unit mean. The noise at each node is assumed to be complex additive white Gaussian with zero mean and variance one. The instantaneous received SNR at the legitimate node A_{n+1} and eavesdropper (at position) e in Φ_{ne} can be respectively given as

$$\mathtt{SNR}_n \triangleq \frac{pH_n}{|D_n|^{\alpha}+1}, \tag{1}$$

$$\mathtt{SNR}_{ne} \triangleq \frac{pS_{ne}}{|X_{ne}|^{\alpha}+1}, \tag{2}$$

where p denotes the transmit power at the legitimate node A_n assumed the same in each hop; H_n and $|D_n|$ are the channel power fading gain and the distance between the nth link A_nA_{n+1}, respectively; S_{ne} and $|X_{ne}|$ are the channel power fading gain and the distance between the legitimate node A_n and eavesdropper e, respectively. Since the distance for each hop is the same between the legitimate nodes, the statistics of $\mathtt{SNR}_n$ is the same for all n. Note that we have normalized the receiver noise power to be one, which means that the parameter p in fact represents the transmitter-side SNR instead of the actual transmit power.

We assume non-cooperative eavesdroppers. Then the maximum received SNR, $\mathtt{SNR}_{ne}^{\max}$, at eavesdroppers from the legitimate node A_n is equivalent to $\max\limits_{e\in\Phi_{ne}}\{\mathtt{SNR}_{ne}\}$, where the maximization operation means the selection of the eavesdropper which has the strongest received signal.

B. Transmission Schemes

We consider the well-known Wyner's encoding scheme [23]. The transmitters encode the message using two rate parameters, namely, the rate of the transmitted codewords R_t and the rate of the confidential information R_s. The rate difference $R_e \triangleq R_t - R_s$ represents the rate loss for transmitting the message securely against eavesdropping

which reflects the ability of securing the message transmission against eavesdropping [24]. We assume that the intermediate relay nodes use the RaF relaying protocol which is specifically designed from the viewpoint of physical layer security. RaF relaying deviates from the widely-used DF relaying in the way that the relays use independent codewords to add independent randomization in each hop when re-encoding the received signal [14]. We consider fixed-rate transmission, hence R_t and R_s are designed offline. This is a commonly-adopted practical assumption as its implementation is based on long-term channel statistics and does not require instantaneous feedback of the full channel state information (CSI) for every hop. For reducing the risk of eavesdropping, we assume that there is no retransmission in each hop. Depending on whether there is feedback from the receiver to the transmitter, we can have the following two transmission schemes: OFT and NOFT, as described below.

For a given transmission rate R_t, the receiver is able to decode the transmission if the instantaneous received SNR exceeds a threshold β_t, where $\beta_t = 2^{R_t} - 1$. Assuming the receiver has perfect channel knowledge (e.g., obtained from pilot transmissions), it is possible for the receiver to feed back to the transmitter some information about its channel status. In the OFT scheme [24], we assume that the receiver uses a one-bit feedback (as opposed to full CSI feedback) to inform the transmitter whether the instantaneous received SNR exceeds β_t or not. Transmission is suspended if the received SNR falls below β_t. Then, the transmission probability of the nth hop can be defined as

$$\mathcal{P}_t^{'} \triangleq \mathcal{P}\left(\mathtt{SNR}_n > \beta_t\right). \tag{3}$$

Since the statistics of $\mathtt{SNR}_n$ is the same for all n, $\mathcal{P}_t^{'}$ is the same for all hops. Although the transmission suspension causes delay as reflected in the transmission probability, it guarantees successful connection/decoding for each hop whenever transmission happens.

If there is no feedback, i.e., in the NOFT scheme, there is no suspension of transmission, and hence, the transmission probability is $\mathcal{P}_t^{'} = 1$. However, the receiver may not be able to decode. Specifically, the connection probability (i.e., the probability that the receiver is able to decode the message) of the nth hop is defined as

$$\mathcal{P}_c^{'} \triangleq \mathcal{P}\left(\mathtt{SNR}_n > \beta_t\right). \tag{4}$$

Hence, the end-to-end connection probability of the path in the NOFT scheme is given by

$$\mathcal{P}_{\mathrm{c}} \triangleq \mathcal{P}\left(\min_{n=1,\ldots,N}\left\{\mathtt{SNR}_n\right\} > \beta_t\right). \tag{5}$$

For any given R_t and R_s, the secrecy outage probability of the nth hop is defined as [24]

$$\mathcal{P}_{\mathrm{so}}^{'} = \mathcal{P}\left(C_{\mathrm{ne}}^{\max} > R_t - R_s\right) = \mathcal{P}\left(\mathtt{SNR}_{ne}^{\max} > \beta_e\right), \tag{6}$$

where $C_{\mathrm{ne}}^{\max}$ is the maximum capacity of the eavesdroppers' channels in the nth hop and $\beta_e = 2^{R_e} - 1$.

Because the relays apply the RaF protocol, the source and relays use different codewords to transmit the secret message. According to [14], the message is secure when every hop in the path is secure. Hence, the end-to-end secrecy outage probability of the path can be expressed as

$$\mathcal{P}_{\mathrm{so}} \triangleq \mathcal{P}\left(\max_{n=1,\ldots,N}\left\{\mathtt{SNR}_{ne}^{\max}\right\} > \beta_e\right). \tag{7}$$

Furthermore, we assume that the point processes $\Phi_{ne}\,(n = 1, \ldots, N)$ representing the eavesdroppers' locations in different hops are independent, which is a worse case from the view of security compared to the scenario where the eavesdroppers' locations are fixed during all hops. In the next section, we will prove that the secrecy outage probability under the independent point-processes assumption is strictly higher than the secrecy outage probability under the fixed eavesdropper-locations assumption. Because the legitimate nodes have little knowledge on the eavesdroppers' locations or their mobility, it is best to consider a worse case scenario from the security point of view.

Since the statistics of the legitimate link is the same and the fading gains are independent in each hop, the end-to-end connection probability in the NOFT scheme defined in (5) is equivalent to

$$\mathcal{P}_{\mathrm{c}} = \left(\mathcal{P}_{\mathrm{c}}^{'}\right)^N. \tag{8}$$

Clearly the end-to-end connection probability in the OFT scheme is 1, but this is at the price of the reduced transmission probability as described in (3).

For both NOFT and OFT schemes, the end-to-end secrecy outage probability defined in (7) is equivalent to

$$\mathcal{P}_{\mathrm{so}} = 1 - \left(1 - \mathcal{P}_{\mathrm{so}}^{'}\right)^N. \tag{9}$$

C. Secure Transmission Throughput

Secure transmission throughput characterizes the spectral efficiency of secure communication in a given multihop path for a source-destination pair of nodes which is defined as the average end-to-end rate of the transmission of confidential messages that can be sustained reliably, normalized by the total transmission time:

$$\mathbb{U} = \frac{\mathcal{P}_t^{'}\mathcal{P}_c R_s}{N}, \tag{10}$$

where $\frac{N}{\mathcal{P}_t^{'}}$ is the total expected transmission time (in slots) for transmitting a confidential message from source to destination which includes the transmission time and waiting time along the path; $\mathcal{P}_c$ represents the probability that a confidential message is transmitted correctly from the source to the destination over the path. Secure transmission throughput shows the dependence of the network spectral efficiency on the key system parameters, e.g., the transmission rate parameters, the number of hops, the transmit power, and the density of eavesdroppers.

As explained before, in the NOFT scheme, the transmission probability of a single hop $\mathcal{P}_t^{'} = 1$ and the total expected transmission time is N. Then, secure transmission throughput can be rewritten as $\mathbb{U} = \frac{\mathcal{P}_c R_s}{N}$, which is the same as the definition of secure transmission throughput in [25–27]. On the other hand, in the OFT scheme, the connection probability

of the path $\mathcal{P}_{\rm c}=1$ and the total expected transmission time is $\frac{N}{\mathcal{P}_t^{'}}$. Then, secure transmission throughput can be rewritten as $\mathbb{U}=\frac{\mathcal{P}_t^{'}R_s}{N}$, which is the same as the definition of secure transmission throughput in [24]. Hence, our throughput metric is consistent with existing work in this area. We will use the secure transmission throughput as the main performance metric in this paper. Note that the throughput definition in (10) alone does not directly describe the secrecy performance in terms of the secrecy outage probability. We use the end-to-end secrecy outage probability in (7) to directly quantify the level of security for the multihop communication.

III. Secure Transmission Design in a Multihop Path

In this section, we analytically study the secrecy outage performance of a given multihop path of a source-destination pair of nodes. Then, for both OFT and NOFT schemes, we consider the secure transmission design to maximize secure transmission throughput under the secrecy outage constraint.

A. Secrecy Performance and Throughput Maximization Problem

In this subsection, we derive an explicit expression of the end-to-end secrecy outage probability. Then, we formulate the throughput maximization problem by the joint design of the number of hops, the rate of the transmitted codewords and the rate of the confidential information.

Theorem 1: The end-to-end secrecy outage probability of the path for both NOFT and OFT schemes is given by

$$\mathcal{P}_{\rm so}=1-\exp\left[-NK_1\left(\frac{\beta_e}{p}\right)^{-\frac{2}{\alpha}}\exp\left[-\frac{\beta_e}{p}\right]\right], \qquad (11)$$

where $K_1=\pi\lambda_e\Gamma\left(\frac{2}{\alpha}+1\right)$ and $\Gamma(\cdot)$ is the gamma function.

Proof: See Appendix A. ∎

Now we revisit the assumption on the eavesdroppers' location made in Section II-A and provide a justification for it. In particular, we have assumed that the eavesdroppers' locations change independently from hop to hop. Of course, this assumption does not accurately reflect the realistic locations of eavesdroppers, unless they have extremely high mobility. Without any knowledge of the eavesdroppers' locations and mobility, however, we have to make some assumption in order to assess the network performance. In the following corollary, we show that the assumption adopted in this work is more robust than assuming that the eavesdropper locations are fixed over all hops (i.e., stationary eavesdroppers).

Corollary 1: The secrecy outage probability under the independent point-processes assumption is strictly higher than the secrecy outage probability under the fixed eavesdropper-locations assumption.

Proof: See Appendix B. ∎

The result in Corollary 1 agrees with intuition because that the eavesdroppers under the independent point-processes assumption have more degrees of freedom than the eavesdroppers under the fixed locations assumption, that is, more variation in the locations gives eavesdroppers more chance to cause secrecy problem to at least one of the hops. Hence, when not knowing the exact locations or mobility of the eavesdroppers, it is more appropriate for the designers of the legitimate network to consider a worse-case scenario, i.e., the independent point-processes assumption adopted in this work.

With the end-to-end secrecy outage probability derived in Theorem 1 to quantify the secrecy performance, we now formulate a network design problem of maximizing the secure transmission throughput subject to a given secrecy requirement:

$$\max_{R_t,R_s,N}\ \mathbb{U}=\frac{\mathcal{P}_t^{'}\mathcal{P}_c R_s}{N},\quad s.t.\ \mathcal{P}_{\rm so}\le\epsilon,$$

where $\epsilon\in[0,1]$ represents the minimum security requirement. The controllable design parameters are the rate of the transmitted codewords R_t, the rate of the confidential information R_s, and the number of hops N of the path.

B. On-Off Transmission Scheme

We first consider the OFT scheme, i.e., transmission occurs whenever the received SNR at the legitimate node exceeds the SNR threshold β_t. Hence, for any transmitted message, the legitimate receiver is able to decode correctly, i.e., the end-to-end connection probability of the path $\mathcal{P}_{\rm c}=1$.

According to (1) and (3), the transmission probability can be computed as

$$\mathcal{P}_t^{'}=\mathcal{P}\left(\frac{pH_n}{\left(\frac{L}{N}\right)^{\alpha}+1}>\beta_t\right)=\exp\left[\frac{-\beta_t\left[\left(\frac{L}{N}\right)^{\alpha}+1\right]}{p}\right]. \qquad (12)$$

Now, we consider the design problem of maximizing secure transmission throughput by the joint design of R_t, R_s and N, expressed as

$$\begin{aligned}\textbf{P1}:\ \max_{R_t,R_s,N}\quad & \mathbb{U}=\frac{\mathcal{P}_t^{'}(R_t,N)\,R_s}{N}, && (13a)\\ s.t.\quad & \mathcal{P}_{\rm so}(R_t,R_s,N)\le\epsilon, && (13b)\\ & R_t\ge R_s>0, && (13c)\\ & N\ge 1, && (13d)\end{aligned}$$

where we have explicitly shown the dependence of $\mathcal{P}_{\rm so}$ and $\mathcal{P}_t^{'}$ on R_t, R_s and N.

1) The Optimal Rate Parameters R_t and R_s for Fixed Hop-Count N: To solve the above optimization problem **P1**, we first consider the sub-problem that we get the optimal rate parameters R_t and R_s for fixed hop-count N. This sub-problem has its important physical meaning: how to optimally design the encoding rates for a given network setting.

Since the constraint (13b) is satisfied only when the constraint (13c) is satisfied, the constraint (13c) can be simplified as $R_s>0$. Since $\mathcal{P}_t^{'}$ is independent of R_s and $\mathcal{P}_{\rm so}$ is an increasing function of R_s, it is optimal to maximize $\mathcal{P}_{\rm so}$ in

order to maximize R_s in $\mathbb{U}$. Hence, we can obtain the optimal $\mathcal{P}_{\text{so}}$ as

$$\mathcal{P}_{\text{so}}\left(R_t, R_s, N\right) = \epsilon. \tag{14}$$

The value of β_e that satisfies the above equality is given as

$$\beta_e = \frac{2p}{\alpha}\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right), \tag{15}$$

where $\mathbb{W}_0\left(\cdot\right)$ is the principal branch of Lambert W function. Then, from (15), we can derive

$$R_e = R_t - R_s = \log_2\left[\frac{2p}{\alpha}\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right)+1\right]. \tag{16}$$

Under this condition, we can reformulate the optimization problem as

$$\mathbf{P1}': \max_{R_t} \quad \mathbb{U} = \frac{(R_t - R_e)\exp\left[-K_2\left(2^{R_t}-1\right)\right]}{N}, \tag{17a}$$

$$s.t. \quad R_t > R_e, \tag{17b}$$

where $K_2 = \frac{\left[\left(\frac{L}{N}\right)^{\alpha}+1\right]}{p}$; R_e is a function of N, whose explicit expression can be found in (16).

Theorem 2: Secure transmission throughput $\mathbb{U}$ is a quasi-concave function of the rate of the transmitted codewords R_t. Then, the optimal value of R_t and R_s to maximize $\mathbb{U}$ are given as

$$R_t^* = R_e + \frac{1}{\ln 2}\mathbb{W}_0\left(\frac{2^{-R_e}}{K_2}\right), \tag{18}$$

and

$$R_s^* = \frac{1}{\ln 2}\mathbb{W}_0\left(\frac{2^{-R_e}}{K_2}\right). \tag{19}$$

Proof: See Appendix C. ∎

Corollary 2: The optimal rate of the transmitted codewords R_t^* is an increasing function of the number of hop N. And when N goes to infinity, the optimal rate of the confidential information R_s^* approaches 0.

Proof: See Appendix D. ∎

The result in Corollary 2 clearly says that a network with too many hops will lead to no secure throughput, since the drawback of causing more chances for eavesdropping outweighs the benefit of allowing more randomness in the code, i.e. R_s^* goes to 0. Hence, we definitely expect that the optimal number of hops to be finite.

Corollary 3: As p grows to infinity, the optimal value of R_t goes to infinity and the optimal values of R_s and $\mathbb{U}$ converge to constants, given as

$$R_s^* = \frac{1}{\ln 2}\mathbb{W}_0\left(\frac{1}{K_3}\right), \tag{20}$$

and

$$\mathbb{U}^* = \frac{1}{N\ln 2}\mathbb{W}_0\left(\frac{1}{K_3}\right)\exp\left[-K_3\exp\left[\mathbb{W}_0\left(\frac{1}{K_3}\right)\right]\right], \tag{21}$$

where $K_3 = \frac{2}{\alpha}\left[\left(\frac{L}{N}\right)^{\alpha}+1\right]\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right)$.

Proof: See Appendix E. ∎

If there is no secrecy requirement for the system, increasing the transmit power can always increase the throughput. However, for the system with secrecy requirement, the improvement of the throughput tends to zero as the transmit power grows to infinity since increasing power benefits both the legitimate and eavesdropping channels.

2) The Optimal Hop-Count N: With the obtained explicit expressions of R_t^* and R_s^*, in the following, we study how to design the number of hops N of the path. Replacing R_t with (18), then the optimization problem $\mathbf{P1}'$ can be rewritten as:

$$\mathbf{P1}'': \max_{N} \quad \mathbb{U} = \frac{\mathbb{W}_0\left(\frac{2^{-R_e}}{K_2}\right)}{N\ln 2} \times \exp\left[-K_2\left(2^{R_e+\frac{1}{\ln 2}\mathbb{W}_0\left(\frac{2^{-R_e}}{K_2}\right)}-1\right)\right], \tag{22a}$$

$$s.t. \quad N \geq 1, \tag{22b}$$

where R_e and K_2 are functions of N, whose explicit expressions can be found earlier. We can see that the objective function is a complicated function of the argument N, which makes the optimization problem $\mathbf{P1}''$ difficult to be solved. We cannot obtain an explicit expression of the optimal value of N, however, this problem can be solved numerically. Note that N is an integer and the feasible range of N is typically small in practical networks. Therefore, it is of minimal complexity to numerically optimize N. We will present numerical results on the optimal N in Section IV.

C. Non-On-Off Transmission Scheme

We now consider the NOFT scheme. Since there is no feedback of the instantaneous SNR from the receiver to the transmitter, there is no suspension of transmission. Hence, each hop transmits the message instantly without waiting, i.e., the transmission probability of the nth hop $\mathcal{P}_t^{'} = 1$.

According to (1) and (4), the connection probability can be computed as

$$\mathcal{P}_c^{'} = \mathcal{P}\left(\frac{pH_n}{\left(\frac{L}{N}\right)^{\alpha}+1} > \beta_t\right) = \exp\left[\frac{-\beta_t\left[\left(\frac{L}{N}\right)^{\alpha}+1\right]}{p}\right]. \tag{23}$$

Replacing $\mathcal{P}_{\text{c}}^{'}$ with (23) into (8), the end-to-end connection probability of the path can be computed as

$$\mathcal{P}_c = \exp\left[\frac{-N\beta_t\left[\left(\frac{L}{N}\right)^{\alpha}+1\right]}{p}\right]. \tag{24}$$

Now, we consider the design problem of maximizing secure transmission throughput by the joint design of R_t, R_s and N,

expressed as

$$\mathbf{P2}: \max_{R_t,R_s,N} \quad \mathbb{U}=\frac{\mathcal{P}_c\left(R_t,N\right)R_s}{N}, \tag{25a}$$
$$s.t. \quad \mathcal{P}_{\text{so}}\left(R_t,R_s,N\right)\leq\epsilon, \tag{25b}$$
$$R_t\geq R_s>0, \tag{25c}$$
$$N\geq 1, \tag{25d}$$

where we have explicitly shown the dependence of $\mathcal{P}_{\text{so}}$ and $\mathcal{P}_c$ on R_t, R_s and N.

1) The Optimal Rate Parameters R_t and R_s for Fixed Hop-Count N: To solve the above optimization problem **P2**, we first consider the sub-problem that we get the optimal rate parameters R_t and R_s for fixed hop-count N. As explained before, this sub-problem has its important physical meaning: how to optimally design the encoding rates for a given network setting.

Similar to the OFT case, the optimal design needs to satisfy (14). Then, the optimal values of R_t and R_s should satisfy (16).

Under this condition, we can reformulate the optimization problem **P2** as

$$\mathbf{P2}': \max_{R_t} \quad \mathbb{U}=\frac{(R_t-R_e)\exp\left[-K_4\left(2^{R_t}-1\right)\right]}{N}, \tag{26a}$$
$$s.t. \quad R_t>R_e, \tag{26b}$$

where $K_4=\frac{N\left[\left(\frac{L}{N}\right)^{\alpha}+1\right]}{p}$; R_e is a function of N, whose explicit expression can be found in (16).

Theorem 3: Secure transmission throughput $\mathbb{U}$ is a quasi-concave function of the rate of the transmitted codewords R_t. Then, the optimal value of R_t and R_s to maximize $\mathbb{U}$ are given as

$$R_t^*=R_e+\frac{1}{\ln 2}\mathbb{W}_0\left(\frac{2^{-R_e}}{K_4}\right), \tag{27}$$

and

$$R_s^*=\frac{1}{\ln 2}\mathbb{W}_0\left(\frac{2^{-R_e}}{K_4}\right). \tag{28}$$

Proof: See Appendix F. ∎

Comparing with the optimal coding rate parameters for the OFT scheme in Theorem 2, we see that the expressions of R_t^* and R_s^* are very similar between the OFT scheme and the OFT scheme. The only but important difference is between the parameter K_2 and K_4. Specifically, $K_4=NK_2$.

Corollary 4: As p grows to infinity, the optimal value of R_t goes to infinity and the optimal values of R_s and $\mathbb{U}$ converge to constants, given as

$$R_s^*=\frac{1}{\ln 2}\mathbb{W}_0\left(\frac{1}{K_5}\right), \tag{29}$$

and

$$\mathbb{U}^*=\frac{1}{N\ln 2}\mathbb{W}_0\left(\frac{1}{K_5}\right)\exp\left[-K_5\exp\left[\mathbb{W}_0\left(\frac{1}{K_5}\right)\right]\right], \tag{30}$$

where $K_5=\frac{2N}{\alpha}\left[\left(\frac{L}{N}\right)^{\alpha}+1\right]\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right)$.

Proof: See Appendix G. ∎

Again, we see that the throughput improvement from increasing the transmit power vanishes as the transmit power goes large.

2) The Optimal Hop-Count N: With the obtained explicit expressions of R_t^* and R_s^*, in the following, we study how to design the number of hops N of the path. Replacing R_t with (27), then the optimization problem **P2′** can be rewritten as:

$$\mathbf{P2}'': \max_{N} \mathbb{U}=\frac{\mathbb{W}_0\left(\frac{2^{-R_e}}{K_4}\right)}{N\ln 2}\times\exp\left[-K_4\left(2^{R_e+\frac{1}{\ln 2}\mathbb{W}_0\left(\frac{2^{-R_e}}{K_4}\right)}-1\right)\right], \tag{31a}$$
$$s.t. \quad N\geq 1, \tag{31b}$$

where R_e and K_4 are functions of N, whose explicit expressions can be found earlier. Again, this problem is difficult to be solved analytically. Nevertheless, it is of minimal complexity to numerically find the optimal N as explained before.

IV. Numerical Results

In this section, we present numerical results on secure transmission throughput and evaluate how different system parameters impact the secure transmission design. We consider a multihop wireless network in which legitimate nodes are placed uniformly on a line in the center of the network. The source node is placed at the origin and the destination is located at $(50\text{m}, 0)$. The eavesdroppers are randomly distributed according to a uniform distribution in the entire network of size 2000m × 2000m. The eavesdroppers' distribution is independent from hop to hop. Unless otherwise stated, we use the following settings to obtain the numerical results: $L=50\text{m}$, $\epsilon=0.05$, $\lambda_e=10^{-5}$, $\alpha=3$, $p=100\text{dB}$ (which corresponds to a practical (sensor-like device) scenario with transmit power of 0dBm and a receiver noise power of -100dBm). Note that although p is said to denote the transmit power, it actually presents the transmitter-side SNR due to the normalization in the receiver noise power.

A. Performance of Secure Transmission

We first show the impact of different system parameters on the design of the encoding rates as well as the secure transmission throughput.

Fig. 2 presents the secrecy performance of the system under fixed hop-count N versus the transmit power p for the case of OFT scheme. As p increases, the received power at eavesdroppers increases as well. To maintain the same level of secrecy, the legitimate nodes need to increase the randomness in the wiretap code, i.e., R_e, which indirectly requires an increase in R_t. This explains the trend seen in the two subfigures on the left. Also, we see that the slopes of R_t and R_e are the same as p increases above 70dB, which explains why $R_s=R_t-R_e$ is a constant for p above 70dB, hence a constant throughput U, which validates our analysis in Proposition 3. Comparing the throughput with different number of hops, we see that the network with 5 hops performs best among the

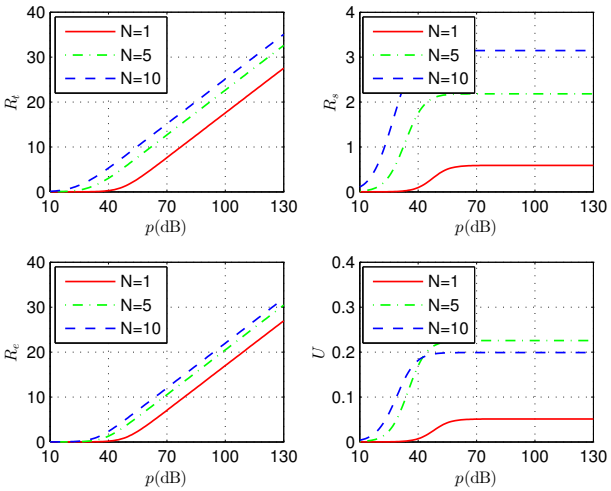


Fig. 2. Performance of secure transmission under fixed hop-count N versus the transmit power p for the case of OFT scheme. The system parameters are $L = 50$m, $\epsilon = 0.05$, $\alpha = 3$, $\lambda_e = 10^{-5}$.

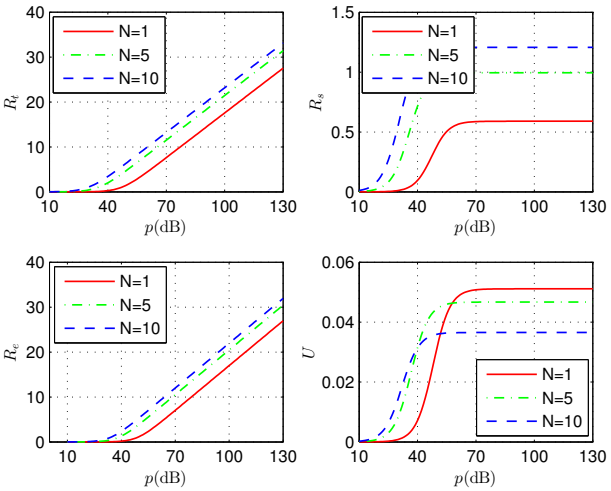


Fig. 3. Performance of secure transmission under fixed hop-count N versus the transmit power p for the case of NOFT scheme. The system parameters are $L = 50$m, $\epsilon = 0.05$, $\alpha = 3$, $\lambda_e = 10^{-5}$.

three different choices of hop-count, indicating that there is an optimal number of hops.

Fig. 3 presents the secrecy performance of the system under fixed hop-count N versus the transmit power p for the case of NOFT scheme. Similar trends are observed as in Fig. 2, hence the results validate Proposition 4. Looking at the throughput sub-figure, we see that the network with a single hop, i.e., direct transmission, performs very well in this case.

Fig. 4 compares the secure transmission throughput between the OFT and NOFT schemes. As expected, the OFT scheme outperforms the NOFT scheme to a large extent. This highlights the importance of implementing the one-bit feedback for the receiver to inform the transmitter about the current channel condition. By focusing on a single curve in the figure, we can find the optimal hop-count in each scheme: the optimal N for the OFT scheme is 5 while the optimal N for the NOFT scheme is 2.

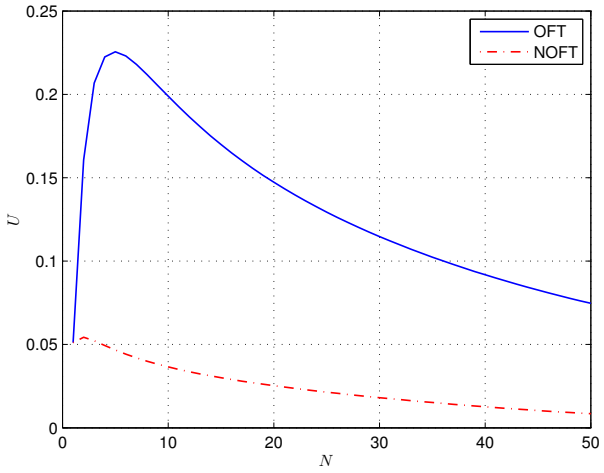


Fig. 4. The secure transmission throughput of both the OFT and NOFT schemes versus hop-count N. The system parameters are $L = 50$m, $\epsilon = 0.05$, $\alpha = 3$, $p = 100$dB, $\lambda_e = 10^{-5}$.

B. Optimal Number of Hops

We now explicitly study the optimal hop-count and the resulting secure transmission throughput.

Fig. 5 presents the optimal hop-count versus the transmit power p. As shown in figure, the hop-count of both the OFT and NOFT schemes decrease as the transmission power p increases. This is somewhat intuitive because more transmit power means less hops needed for the end-to-end communication. In addition, more transmit power means better received signal quality at the eavesdroppers for each hop. To avoid the degradation in secrecy, less number of hop (i.e., less number of transmissions) is desired. It is also important to note that the optimal hop-count quickly reaches a constant as p increases. For example, the optimal N reaches and stays at 5 when $p = 50$dB for the OFT scheme and it reaches and stays at 2 when $p = 55$dB for the NOFT scheme. It is worth mentioning that the practical range of p is orders of magnitude higher than 50dB. For example, $p = 100$dB is a practical value for sensor-like device with a transmit power of 0dBm and a receiver noise power of -100dBm. Therefore, for practical purposes, we expect that the optimal number of hops are very stable and insensitive to the change in the transmit power. Fig. 6 presents the secure transmission throughput achieved using the optimal hop-count. Again, we see that the throughput is constant for practical ranges of p. The secrecy performance of OFT scheme is always better than that of the NOFT scheme.

Fig. 7 presents the optimal hop-count N versus the density of the eavesdropper λ_e. As the density of the eavesdropper λ_e increases, the optimal number of hops increases. This is not intuitive to understand because more hops means more chances for eavesdropping. The reason why having more hops does not degrade secrecy is due to the fact that more hops reduces the distance of communication among the legitimate nodes which in turn allows a much larger randomness to be added into the wiretap code to fight against eavesdropping while still achieving the same level of communication performance. In short, the

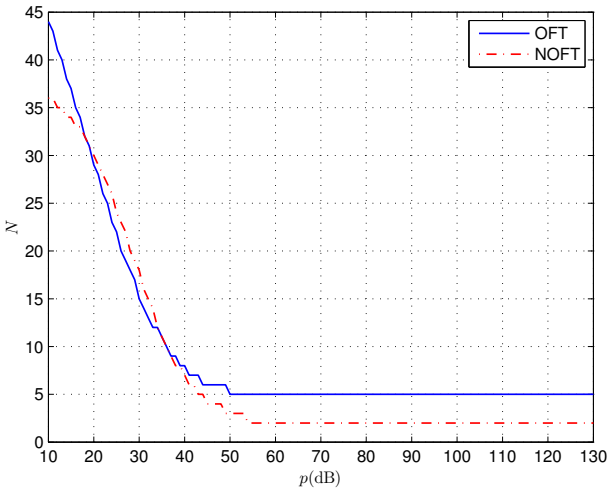


Fig. 5. The optimal hop-count N versus the transmit power p. The system parameters are $L = 50$m, $\epsilon = 0.05$, $\alpha = 3$, $\lambda_e = 10^{-5}$.

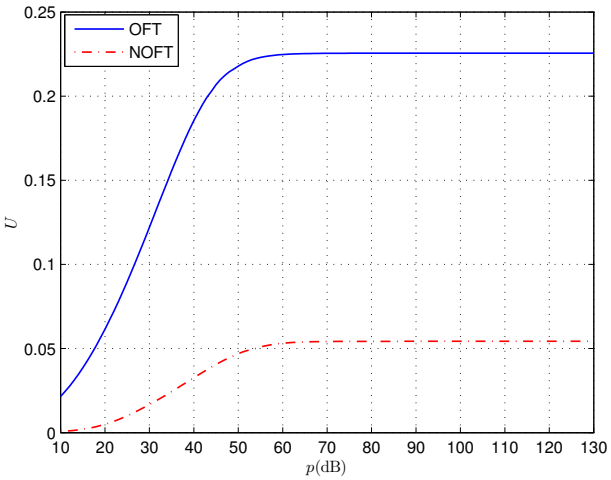


Fig. 6. The optimal secure transmission throughput U versus the transmit power p. The system parameters are $L = 50$m, $\epsilon = 0.05$, $\alpha = 3$, $\lambda_e = 10^{-5}$.

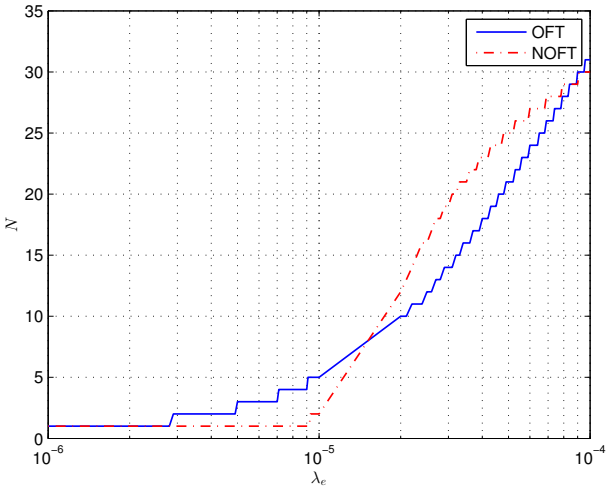


Fig. 7. The optimal hop-count N versus the density of the eavesdropper λ_e. The system parameters are $L = 50$m, $\epsilon = 0.05$, $\alpha = 3$, $p = 100$dB.

benefit of allowing more randomness in the code outweighs the drawback of causing more chances for eavesdropping. Fig. 8 presents the secure transmission throughput achieved by using the optimal hop-count versus the density of the eavesdropper. When the density of eavesdroppers is very low, the NOFT scheme performs as good as the OFT scheme. When more eavesdroppers are present, the performance of NOFT quickly degrades and becomes much worse than the OFT scheme.

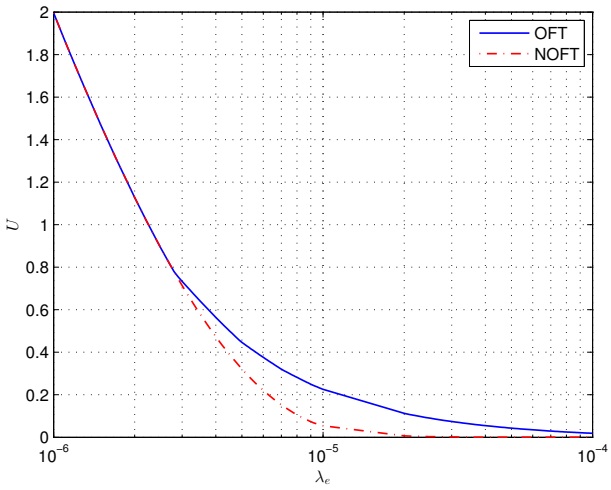


Fig. 8. The optimal secure transmission throughput U versus the density of the eavesdropper λ_e. The system parameters are $L = 50$m, $\epsilon = 0.05$, $\alpha = 3$, $p = 100$dB.

V. Conclusion

In this paper, we investigated the secure transmission problem in a linear multihop network with the help of the relays using randomize-and-forward (RaF) relaying strategy in the presence of randomly distributed eavesdroppers. Under an end-to-end secrecy outage probability constraint, we formulated the design problem of maximizing secure transmission throughput by the joint design of the number of hops and the rate parameters of the wiretap code. Both an on-off transmission (OFT) scheme and a non-on-off transmission (NOFT) scheme were studied. Our results give insights into the impact of the system parameters on the secure transmission throughput. For practical ranges of SNR, we observed that the optimal number of hops as well as the secure transmission throughput remains constant and does not change if more transmit power is used. Our results provide design guidelines for determining the best transmission strategy and the best network configuration in a linear multihop network.

Appendix A
Proof of Theorem 1

According to (2) and (6), the secrecy outage probability of the nth hop for both NOFT and OFT schemes can be computed

as

$$\begin{aligned}\mathcal{P}_{\text{so}}^{'} &= \mathcal{P}\left(\mathtt{SNR}_{ne}^{\max} > \beta_e\right) \\ &= \mathcal{P}\left(\max_{e\in\Phi_{ne}}\left\{\frac{pS_{ne}}{|X_{ne}|^{\alpha}+1}\right\} > \beta_e\right) \\ &= 1 - \mathbb{E}_{\Phi_{ne}}\left[\prod_{e\in\Phi_{ne}}\left\{1-\exp\left[-\frac{\beta_e(|X_{ne}|^{\alpha}+1)}{p}\right]\right\}\right].\end{aligned} \tag{32}$$

According to [28], the probability generating functional (PGFL) for a homogeneous PPP is given as

$$\mathbb{E}_{\Phi_e}\left[\prod_{e\in\Phi_e} f(e)\right] = \exp\left[-\lambda_e\int_{\mathbb{R}^2} 1-f(e)\,\mathrm{d}e\right]. \tag{33}$$

Using (33), (32) can be rewritten as

$$\mathcal{P}_{\text{so}}^{'} = 1-\exp\left[-\lambda_e\int_{\mathbb{R}^2}\exp\left[-\frac{\beta_e(|X_{ne}|^{\alpha}+1)}{p}\right]\mathrm{d}e\right]. \tag{34}$$

Changing to polar coordinates, (34) can be turned to

$$\mathcal{P}_{\text{so}}^{'} = 1-\exp\left[-2\pi\lambda_e\int_0^{+\infty}\exp\left[-\frac{\beta_e({r_e}^{\alpha}+1)}{p}\right]r_e\,\mathrm{d}r_e\right]. \tag{35}$$

Then, (35) can be computed as

$$\mathcal{P}_{\text{so}}^{'} = 1-\exp\left[-K_1\left(\frac{\beta_e}{p}\right)^{-\frac{2}{\alpha}}\exp\left[-\frac{\beta_e}{p}\right]\right]. \tag{36}$$

Replacing $\mathcal{P}_{\text{so}}^{'}$ with (36) into (9), the end-to-end secrecy outage probability of the path can be computed as

$$\mathcal{P}_{\text{so}} = 1-\exp\left[-NK_1\left(\frac{\beta_e}{p}\right)^{-\frac{2}{\alpha}}\exp\left[-\frac{\beta_e}{p}\right]\right]. \tag{37}$$

This completes the proof.

Appendix B
Proof of Corollary 1

We denote the locations of the eavesdroppers in the fixed eavesdroppers case by Φ_e. Then, the end-to-end secrecy outage probability of the path can be expressed as

$$\begin{aligned}\mathcal{P}_{\text{so\_fixed}} =& \mathcal{P}\left(\max_{e\in\Phi_e}\left\{\max_{n=1,\ldots,N}\{\mathtt{SNR}_{ne}\}\right\} > \beta_e\right) \\ =& 1-\mathcal{P}\left(\max_{e\in\Phi_e}\left\{\max_{n=1,\ldots,N}\{\mathtt{SNR}_{ne}\}\right\} < \beta_e\right) \\ =& 1-\mathbb{E}_{\Phi_e}\left[\prod_{e\in\Phi_e}\prod_{n=1}^{N}\left\{1-\exp\left[-\frac{|X_{ne}|^{\alpha}+1}{p/\beta_e}\right]\right\}\right].\end{aligned} \tag{38}$$

Using PGFL (33), (38) can be rewritten as

$$\mathcal{P}_{\text{so\_fixed}} = 1-\exp\left[-\lambda_e\int_{\mathbb{R}^2} 1-\prod_{n=1}^{N}\left(1-\exp\left[-\frac{\beta_e(|X_{ne}|^{\alpha}+1)}{p}\right]\right)\mathrm{d}e\right]. \tag{39}$$

Lemma 1: Let $0 < a_k\,(k=1,2,\ldots,n) < 1$ be arbitrary positive constants. For an arbitrary positive integer n,

$$\prod_{k=1}^{n}(1-a_k) \geq 1-\sum_{k=1}^{n}a_k. \tag{40}$$

Proof: We assume $f_n = \prod_{k=1}^{n}(1-a_k)$ and $g_n = 1-\sum_{k=1}^{n}a_k$. Then, when $n=1$, $f_1 = g_1 = 1-a_1$. When $n=2$, $f_2 - g_2 = a_1a_2 > 0$.

We assume $f_j - g_j > 0$ when $n=j$. Then, when $n=j+1$, we have

$$\begin{aligned}f_{j+1} &= \prod_{k=1}^{j+1}(1-a_k) \\ &> g_j(1-a_{j+1}) \\ &= g_{j+1} + a_{j+1}\sum_{k=1}^{j}a_k \\ &> g_{j+1}.\end{aligned} \tag{41}$$

So we can conclude that f_n is greater than g_n for an arbitrary positive $n \geq 1$. ■

Applying Lemma 1, we can obtain an upper bound of (39) given as

$$\begin{aligned}\mathcal{P}_{\text{so\_fixed}} &\leq 1-\exp\left[-\lambda_e\int_{\mathbb{R}^2}\sum_{n=1}^{N}\exp\left[-\frac{|X_{ne}|^{\alpha}+1}{p/\beta_e}\right]\mathrm{d}e\right] \\ &= 1-\exp\left[-NK_1\left(\frac{\beta_e}{p}\right)^{-\frac{2}{\alpha}}\exp\left[-\frac{\beta_e}{p}\right]\right] = \mathcal{P}_{\text{so}}.\end{aligned} \tag{42}$$

This completes the proof.

Appendix C
Proof of Theorem 2

The first derivative of $\mathbb{U}$ w.r.t. R_t is computed as:

$$\frac{\mathrm{d}\mathbb{U}}{\mathrm{d}R_t} = \frac{\left[1-\ln 2\;K_2\;2^{R_t}\,(R_t-R_e)\right]\exp\left[-K_2\left(2^{R_t}-1\right)\right]}{N}. \tag{43}$$

Let the first derivative equal to zero, i.e.,

$$1-\ln 2\;K_2\;2^{R_t}\,(R_t-R_e) = 0. \tag{44}$$

The value of R_t that satisfies the above equality is given as

$$R_t = R_e + \frac{1}{\ln 2}\mathbb{W}_0\left(\frac{2^{-R_e}}{K_2}\right). \tag{45}$$

Also, the second derivative of $\mathbb{U}$ w.r.t. R_t is computed as:

$$\begin{aligned}\frac{\mathrm{d}^2\mathbb{U}}{\mathrm{d}{R_t}^2} =& \frac{\ln 2\;K_2\;2^{R_t}}{N}\exp\left[-K_2\left(2^{R_t}-1\right)\right] \\ &\times\left[-2-\ln 2\,(R_t-R_e)\left(2^{R_t}K_2-1\right)\right].\end{aligned} \tag{46}$$

Replacing R_t with (45), (46) can be rewritten as

$$\frac{\mathrm{d}^2\mathbb{U}}{\mathrm{d}{R_t}^2} = \frac{\ln 2\ K_2\ 2^{R_e+\frac{1}{\ln 2}\mathbb{W}_0\left(\frac{2^{-R_e}}{K_2}\right)}}{N} \times \exp\left[-K_2\left(2^{R_e+\frac{1}{\ln 2}\mathbb{W}_0\left(\frac{2^{-R_e}}{K_2}\right)}-1\right)\right] \times \left(-1-\mathbb{W}_0\left(\frac{2^{-R_e}}{K_2}\right)\right) < 0. \quad (47)$$

Thus $\mathbb{U}$ is quasi-concave in R_t. Since $\frac{1}{\ln 2}\mathbb{W}_0\left(\frac{2^{-R_e}}{K_2}\right) > 0$ is satisfied, we can easily obtain that the constraint (17b) is also satisfied. Hence, the obtained value of R_t is optimal to maximize $\mathbb{U}$.

Also, combining (16) and (45), the optimal value of R_s to maximize $\mathbb{U}$ can be computed as

$$R_s = \frac{1}{\ln 2}\mathbb{W}_0\left(\frac{2^{-R_e}}{K_2}\right). \quad (48)$$

This completes the proof.

Appendix D
Proof of Corollary 2

From the explicit expression of R_t^*, it is not so intuitive to derive the conclusion. In the following, we show the detail procedure of the proof.

Since $\mathbb{W}_0(x)$ is an increasing function of x when $x > 0$, we can easily derive that R_e is also an increasing function of N from the explicit expression of R_e (16).

Lemma 2: Let $0 < C$ be an arbitrary positive constant. Then $\mathbb{Y} = \mathbb{W}_0\left(\frac{1}{C*z}\right) + \ln(z)$ is an increasing function of z when $z > 0$.

Proof: The first derivative of $\mathbb{Y}$ w.r.t. z is computed as:

$$\frac{\mathrm{d}\mathbb{Y}}{\mathrm{d}z} = \frac{1}{z + z * \mathbb{W}_0\left(\frac{1}{C*z}\right)} > 0. \quad (49)$$

So $\mathbb{Y}$ is an increasing function of z when $z > 0$. ■

Applying Lemma 2, we can obtain that R_t^* is an increasing function of R_e by replacing $z = 2^{R_e}$ and $C = K_2$ in $\mathbb{Y}$.

Since K_2 is an decreasing function of N, then we can conclude that R_t is an increasing function of N.

When $N \to +\infty$, $R_e \to +\infty$ and $K_2 = \frac{1}{p}$. Then

$$R_s^* = R_t^* - R_e = \frac{1}{\ln 2}\mathbb{W}_0(0) = 0. \quad (50)$$

This completes the proof.

Appendix E
Proof of Corollary 3

Replacing R_e and K_2, (19) can be rewritten as

$$R_s^* = \frac{1}{\ln 2}\mathbb{W}_0\left(\frac{p}{\left[\left(\frac{L}{N}\right)^\alpha+1\right]\left[p\frac{2}{\alpha}\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right)+1\right]}\right). \quad (51)$$

As $p \to +\infty$, (51) can be simplified as

$$R_s^* = \frac{1}{\ln 2}\mathbb{W}_0\left(\frac{1}{\frac{2}{\alpha}\left[\left(\frac{L}{N}\right)^\alpha+1\right]\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right)}\right), \quad (52)$$

which is a constant. With this result, it is easy to see that $R_t^* \to +\infty$ as $p \to +\infty$ because $R_e \to +\infty$ as $p \to +\infty$.

Also, the transmission probability $\mathcal{P}_t^{'}$ can be rewritten as

$$\mathcal{P}_t^{'} = \exp\left[-K_2 2^{R_s^*+R_e} - K_2\right]. \quad (53)$$

When $p \to +\infty$,

$$K_2 2^{R_e} = \frac{\left[\left(\frac{L}{N}\right)^\alpha+1\right]\left[p\frac{2}{\alpha}\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right)+1\right]}{p} = \frac{2}{\alpha}\left[\left(\frac{L}{N}\right)^\alpha+1\right]\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right), \quad (54)$$

$$K_2 = \frac{\left(\frac{L}{N}\right)^\alpha+1}{p} = 0. \quad (55)$$

Then, (53) can be simplified as

$$\mathcal{P}_t^{'} = \exp\left[-\frac{2}{\alpha}\left[\left(\frac{L}{N}\right)^\alpha+1\right]\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right) \times \exp\left[\mathbb{W}_0\left(\frac{1}{\frac{2}{\alpha}\left[\left(\frac{L}{N}\right)^\alpha+1\right]\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right)}\right)\right]\right]. \quad (56)$$

Hence, throughput $\mathbb{U}^*$ can be expressed as

$$\mathbb{U}^* = \frac{1}{N\ln 2}\mathbb{W}_0\left(\frac{1}{\frac{2}{\alpha}\left[\left(\frac{L}{N}\right)^\alpha+1\right]\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right)}\right) \times \exp\left[-\frac{2}{\alpha}\left[\left(\frac{L}{N}\right)^\alpha+1\right]\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right) \times \exp\left[\mathbb{W}_0\left(\frac{1}{\frac{2}{\alpha}\left[\left(\frac{L}{N}\right)^\alpha+1\right]\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right)}\right)\right]\right]. \quad (57)$$

This completes the proof.

Appendix F
Proof of Theorem 3

According to Theorem 2, we can derive that secure transmission throughput $\mathbb{U}$ is a quasi-concave function of the rate of the transmitted codewords R_t by replacing K_2 with K_4. Then, the optimal value of R_t and R_s to maximize $\mathbb{U}$ are given as

$$R_t^* = R_e + \frac{1}{\ln 2}\mathbb{W}_0\left(\frac{2^{-R_e}}{K_4}\right), \quad (58)$$

and

$$R_s^* = \frac{1}{\ln 2}\mathbb{W}_0\left(\frac{2^{-R_e}}{K_4}\right). \tag{59}$$

This completes the proof.

Appendix G
Proof of Corollary 4

Replacing R_e and K_4, (28) can be rewritten as

$$R_s^* = \frac{1}{\ln 2}\mathbb{W}_0\left(\frac{p}{N\left[\left(\frac{L}{N}\right)^{\alpha}+1\right]\left[p\frac{2}{\alpha}\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right)+1\right]}\right). \tag{60}$$

As $p \to +\infty$, (60) can be simplified as

$$R_s^* = \frac{1}{\ln 2}\mathbb{W}_0\left(\frac{1}{\frac{2N}{\alpha}\left[\left(\frac{L}{N}\right)^{\alpha}+1\right]\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right)}\right), \tag{61}$$

which is a constant. With this result, it is easy to see that $R_t^* \to +\infty$ as $p \to +\infty$ because $R_e \to +\infty$ as $p \to +\infty$.

Also, the transmission probability $\mathcal{P}_t^{'}$ can be rewritten as

$$\mathcal{P}_t^{'} = \exp\left[-K_4 2^{R_s^*+R_e} - K_4\right]. \tag{62}$$

When $p \to +\infty$,

$$\begin{aligned} K_4 2^{R_e} &= \frac{N\left[\left(\frac{L}{N}\right)^{\alpha}+1\right]\left[p\frac{2}{\alpha}\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right)+1\right]}{p} \\ &= \frac{2N}{\alpha}\left[\left(\frac{L}{N}\right)^{\alpha}+1\right]\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right), \end{aligned} \tag{63}$$

$$K_4 = \frac{N\left[\left(\frac{L}{N}\right)^{\alpha}+1\right]}{p} = 0. \tag{64}$$

Then, (62) can be simplified as

$$\begin{aligned} \mathcal{P}_t^{'} = \exp&\left[-\frac{2N}{\alpha}\left[\left(\frac{L}{N}\right)^{\alpha}+1\right]\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right)\right. \\ &\left.\times\exp\left[\mathbb{W}_0\left(\frac{1}{\frac{2N}{\alpha}\left[\left(\frac{L}{N}\right)^{\alpha}+1\right]\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right)}\right)\right]\right]. \end{aligned} \tag{65}$$

Hence, throughput $\mathbb{U}^*$ can be expressed as

$$\begin{aligned} \mathbb{U}^* = &\frac{1}{N\ln 2}\mathbb{W}_0\left(\frac{1}{\frac{2N}{\alpha}\left[\left(\frac{L}{N}\right)^{\alpha}+1\right]\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right)}\right) \\ &\times\exp\left[-\frac{2N}{\alpha}\left[\left(\frac{L}{N}\right)^{\alpha}+1\right]\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right)\right. \\ &\left.\times\exp\left[\mathbb{W}_0\left(\frac{1}{\frac{2N}{\alpha}\left[\left(\frac{L}{N}\right)^{\alpha}+1\right]\mathbb{W}_0\left(\frac{\alpha}{2}\left[\frac{\ln\frac{1}{1-\epsilon}}{NK_1}\right]^{-\frac{\alpha}{2}}\right)}\right)\right]\right]. \end{aligned} \tag{66}$$

This completes the proof.

References

[1] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[2] T.-X. Zheng, H.-M. Wang, F. Liu, and M. H. Lee, "Outage constrained secrecy throughput maximization for DF relay networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1741–1755, May 2015.

[3] C. Cai, Y. Cai, X. Zhou, W. Yang, and W. Yang, "When does relay transmission give a more secure connection in wireless ad hoc networks?" *IEEE Trans. Inf. Foren. Sec.*, vol. 9, no. 4, pp. 624–632, Apr. 2014.

[4] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 878–881, Jun. 2012.

[5] W. Saad, X. Zhou, B. Maham, T. Basar, and H. Poor, "Tree formation with physical layer security considerations in wireless multi-hop networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 11, pp. 3980–3991, Nov. 2012.

[6] A. Sheikholeslami, M. Ghaderi, H. Pishro-Nik, and D. Goeckel, "Energy-efficient routing in wireless networks in the presence of jamming," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6828–6842, Oct. 2016.

[7] M. Ghaderi, D. Goeckel, A. Orda, and M. Dehghan, "Minimum energy routing and jamming to thwart wireless network eavesdroppers," *IEEE Trans. Mobile Comput.*, vol. 14, no. 7, pp. 1433–1448, Jul. 2015.

[8] X. He and A. Yener, "End-to-end secure multi-hop communication with untrusted relays," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 1–11, Jan. 2013.

[9] J. H. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 525–528, Apr. 2015.

[10] J. Yao, S. Feng, X. Zhou, and Y. Liu, "Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 753–764, Feb. 2016.

[11] S. Tomasin, "Routing over multi-hop fading wiretap networks with secrecy outage probability constraint," *IEEE Commun. Lett.*, vol. 18, no. 10, pp. 1811–1814, Oct. 2014.

[12] H. Moosavi and F. M. Bui, "Delay-aware optimization of physical layer security in multi-hop wireless body area networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 1928–1939, Sep. 2016.

[13] P. H. J. Nardelli, H. Alves, C. H. M. D. Lima, and M. Latva-Aho, "Throughput maximization in multi-hop wireless networks under a secrecy constraint," *Computer Networks*, vol. 109, pp. 13–20, Nov. 2016.

[14] O. Koyluoglu, C. Koksal, and H. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.

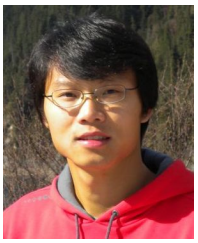
[15] O. Waqar, M. A. Imran, M. Dianati, and R. Tafazolli, "Energy consumption analysis and optimization of BER-constrained amplify-and-forward relay networks," *IEEE Trans. Veh. Technol.*, vol. 63, no. 3, pp. 1256–1269, Mar. 2014.

[16] K. Stamatiou and M. Haenggi, "Delay characterization of multihop transmission in a poisson field of interference," *IEEE/ACM Trans. Networking*, vol. 22, no. 6, pp. 1794–1807, Dec. 2014.

[17] M. Sikora, J. N. Laneman, M. Haenggi, D. J. Costello, and T. E. Fuja, "Bandwidth- and power-efficient routing in linear wireless networks," *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2624–2633, Jun. 2006.

[18] Z. Guan, T. Melodia, and G. Scutari, "To transmit or not to transmit? distributed queueing games in infrastructureless wireless networks," *IEEE/ACM Trans. Networking*, vol. 24, no. 2, pp. 1153–1166, Apr. 2016.
[19] A. Guo and M. Haenggi, "Asymptotic deployment gain: A simple approach to characterize the SINR distribution in general cellular networks," *IEEE Trans. Commun.*, vol. 63, no. 3, pp. 962–976, Mar. 2015.
[20] R. Giacomelli, R. K. Ganti, and M. Haenggi, "Outage probability of general ad hoc networks in the high-reliability regime," *IEEE/ACM Trans. Networking*, vol. 19, no. 4, pp. 1151–1163, Aug. 2011.
[21] R. K. Ganti and M. Haenggi, "Spatial analysis of opportunistic downlink relaying in a two-hop cellular system," *IEEE Trans. Commun.*, vol. 60, no. 5, pp. 1443–1450, May 2012.
[22] S. A. R. Zaidi, D. C. McLernon, and M. Ghogho, "Correction to mobile crowd-sensing wireless activity with measured interference power[oct 13 539-542]," *IEEE Wireless Commun. Lett.*, vol. 4, no. 3, pp. 341–343, Jun. 2015.
[23] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[24] X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.
[25] X. Zhou, R. Ganti, J. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.
[26] J. G. Andrews, S. Weber, M. Kountouris, and M. Haenggi, "Random access transport capacity," *IEEE Trans. Wireless Commun.*, vol. 9, no. 6, pp. 2101–2111, Jun. 2010.
[27] Y. Chen and J. G. Andrews, "An upper bound on multihop transmission capacity with dynamic routing selection," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3751–3765, Jun. 2012.
[28] S. N. Chiu, D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic geometry and its applications*. John Wiley & Sons, 2013.

Jianping Yao received the B.E. degree in communication of engineering from Guangdong University of Technology, Guangzhou, China, in 2010 and the M.E. and Ph.D. degrees in information and communication of engineering from South China University of Technology, Guangzhou, China, in 2013 and 2017, respectively. His research interests include physical layer security, full-duplex and stochastic geometry in multihop wireless networks.



Xiangyun Zhou (SM'17) is a Senior Lecturer at the Australian National University (ANU). He received the Ph.D. degree from ANU in 2010. His research interests are in the fields of communication theory and wireless networks. He currently serves on the editorial board of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and IEEE COMMUNICATIONS LETTERS. He served as a guest editor for IEEE COMMUNICATIONS MAGAZINE's feature topic on wireless physical layer security in 2015. He also served as symposium/track and workshop co-chairs for major IEEE conferences. He was the chair of the ACT Chapter of the IEEE Communications Society and Signal Processing Society from 2013 to 2014. He is a recipient of the Best Paper Award at ICC'11 and IEEE ComSoc Asia-Pacific Outstanding Paper Award in 2016.

Yuan Liu (S'11-M'13) received the B.S. degree from Hunan University of Science and Technology, Xiangtan, China, the M.S. degree from Guangdong University of Technology, Guangzhou, China, and the Ph.D. degree from Shanghai Jiao Tong University, Shanghai, China, all in electronic engineering, in 2006, 2009, and 2013, respectively. Since fall 2013, he has been an Assistant Professor with South China University of Technology, Guangzhou, China. His research interests include wireless communications and networking. He is now an Editor for the IEEE Access.

Suili Feng (M'05) received the B.S. degree in electrical engineering from South China Institute of Technology, Guangzhou, China, in 1982 and the M.S. and Ph.D. degrees in electronic and communication system from South China University of Technology, Guangzhou, China, in 1989 and 1998, respectively. He was a research assistant in Hong Kong Polytechnic University during 1991-1992 and a visiting scholar in University of South Florida during 1998-1999. He has been with South China University of Technology, Guangzhou, China, since 1989, where he currently works as a Professor in the School of Electronic and Information Engineering. His research interests include wireless networks, computer networks and communication signal processing, etc.